Exhibit A

TITLE

METHODS, APPARATUS AND COMPUTER PROGRAM PRODUCTS FOR SECURELY ACCESSING ACCOUNT DATA

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to, and the benefit of, U.S. Provisional Patent Application Serial No. 61/138,711, filed December 18, 2008, which is hereby incorporated by reference in its entirety.

BACKGROUND OF THE INVENTION

Field of the Invention

[0002] The present invention generally relates to securely processing customer account data, and more particularly to a system, computer program product, and method for securely interfacing card issuer databases with a client system tool.

Related Art

[0003] The proliferation of rogue programs such as viruses, trojan horses, and computer hackers, etc., places computing devices at risk. Customer account data which is stored, even temporarily, on a customer's computing device is potentially at risk due to these malicious entities. As a result, customers, merchants, and card issuers are reluctant to utilize tools which reside on a customer computing device and interface with sensitive customer account data.

[0004] Notwithstanding such environments, online shopping through customer computing devices is now just as common as in-store shopping. A payment transaction is typically performed by a customer through a personal computer connected to a public network such as the Internet. Typically, a customer, whether through the merchant's web site or a third party payment processing web site, manually enters his or her account information into fields on a web page to process the transaction. To avoid memorizing information, such as account numbers, and to avoid typing additional information used to make a purchase, some customers use customer account data storage programs. This permits the customer to avoid the tedious task of manually entering this information during each transaction.

Such a program (or devices) is often referred to as a digital wallet or an e-wallet program.

[0005] A digital wallet program allows a customer to store information which can be automatically loaded into a merchant website form which is used to complete a transaction. While digital wallet programs remove the hassle associated with manually entering account information for each transaction, a user still is required to enter some information prior to their initial use.

[0006] One legitimate concern is that the information that is manually or automatically loaded at the customer's device can be exposed to rogue programs running on the customer's computing device. Even if the account data is ultimately stored in an encrypted form, the account data may also be exposed during data entry and prior to encryption by the digital wallet software. Accordingly, card issuers are reluctant to provide customer computing devices access to customer account data.

[0007] Communications between the customer's computing device and card issuer databases are typically encrypted. Once the customer account data is received by the customer computing device, however, the data is decrypted for use by the customer (*e.g.*, viewing or storage) and may then be intercepted, snooped, or otherwise accessed by rogue programs running on the customer's device.

[0008] While customers are able to access recent transactions, payments, and statements through card issuer websites, these interfaces do not provide access to the customer account data required for transaction processing. For instance, typically only the last four digits of a credit card number will be displayed.

[0009] Given the foregoing, one technical challenge is to allow data, such as sensitive customer account data, to be transmitted to a computing device and decrypted within the receiving computing device such that the data is not exposed to malicious entities external or internal to the computing device.

BRIEF DESCRIPTION OF THE INVENTION

[0010] The present invention meets the above-identified needs by providing a system, method and computer program product for securely interfacing card issuer databases with a client system tool.

[0011] In one embodiment a method and computer readable medium are provided for securely downloading customer data to a browser toolbar. Via the browser toolbar, a request for customer data from a customer is received. A check is performed to determine whether the request for customer data includes a request for personal identifiable information requiring encryption by a public encryption key generated by the browser toolbar. The customer is authenticated based on a set of a user credential and an account specific access credential. The user credential and the account specific access credential are distinct, and the account specific access credential is associated with an account of the customer. The requested personal identifiable information is encrypted using the public encryption key generated by the browser toolbar. The encrypted personal identifiable information is transmitted to the browser toolbar.

[0012] In another embodiment, a system for securely integrating personal identifiable information with a browser toolbar unit is provided. The system includes a web interface unit, a toolbar server application, and a transmission unit. The web interface unit is configured to receive, via the browser toolbar, a request for customer data from a customer. The toolbar server application is configured to determine that the request for customer data includes a request for personal identifiable information requiring encryption by a public encryption key generated by the browser toolbar; to authenticate the customer based on a set of a user credential and an account specific access credential; and to encrypt the requested personal identifiable information using the public encryption key generated by the browser toolbar. The user credential and the account specific access credential are distinct, and the account specific access credential is associated with an account of the customer. The transmission unit is configured to transmit the encrypted personal identifiable information to the browser toolbar.

[0013] Further features and advantages of the present invention as well as the structure and operation of various embodiments of the present invention are described in detail below with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] The features and advantages of the present invention will become more apparent from the detailed description set forth below when taken in conjunction with the drawings.

[0015] Figure 1 is a collaboration diagram of functional modules deployed on one or more computer systems for implementing secure access to personal identifiable information in one embodiment of the present invention.

[0016] Figure 2 is a flowchart illustrating a secure personal identifiable information access process in one embodiment of the present invention.

[0017] Figure 3 is a flowchart illustrating the functional modules associated with specific function(s) to securely download personal identifiable information data to a customer's computer in one embodiment of the present invention.

[0018] Figure 4 is a collaboration diagram of functional modules deployed on one or more computer systems for implementing public/private key pair creation in accordance with an embodiment of the present invention.

[0019] Figure 5 is a block diagram of an exemplary computer system useful for implementing the present invention.

DETAILED DESCRIPTION

[0020] The present invention is directed to a system, method and computer program product for securely interfacing card issuer databases with a client system tool. In an exemplary embodiment the client system tool is a web browser toolbar. The toolbar of the present invention allows customers of card issuers to securely manage their account data in environments, such as a customer's computer, which may otherwise be insecure.

[0021] The terms "user," "customer," "cardmember," and/or the plural form of these terms are used interchangeably throughout herein to refer to those persons or

entities capable of accessing, using, being affected by and/or benefiting from the present invention.

[0022] A "merchant" as used herein refers to any person, entity, distributor system, software and/or hardware that is a provider, broker and/or any other entity in the distribution chain of goods or services. For example, a merchant may be a grocery store, a retail store, a travel agency, a service provider, an on-line merchant or the like. The term "vendor" is sometimes used interchangeably with the term "merchant".

[0023] A "card" as used herein refers to both "open cards" and "closed cards." "Open cards" are financial transaction cards that are generally accepted at different merchants. Examples of open cards include the American Express®, Visa®, MasterCard® and Discover® cards, which may be used at many different retailers and other businesses. In contrast, "closed cards" are financial transaction cards that may be restricted to use in a particular store, a particular chain of stores or a collection of affiliated stores. One example of a closed card is a pre-paid gift card that may only be purchased at, and only be accepted at, a clothing retailer, such as The Gap® store.

[0024] An "account" as used herein refers to an account associated with an open account or a closed account system. The account may exist in a physical or non-physical embodiment. For example, an account may be distributed in non-physical embodiments such as an account number, frequent-flyer account, telephone calling account or the like. Furthermore, a physical embodiment of a transaction account may be distributed as a financial instrument.

[0025] A "card issuer" and "issuer" as used herein refer to an organization that issues a transaction account and associated financial instrument (*e.g.*, payment device, transaction card, and the like) to a cardmember. They also are responsible for maintaining details of the cardmember's account including eligibility for services, payments made, charges incurred, and the like.

[0026] An "e-wallet" as used herein refers to any data storage implementation which allows data associated with a customer to be stored and used to make electronic commerce transactions. The term "digital wallet" is also used interchangeably with the term "e-wallet."

[0027] "Personal identifiable information" (PII) as used herein refers to any data that a customer, merchant, card issuer or the like wishes to keep confidential. For example, PII data may include a social security number (SSN), outstanding loan information, credit report information, a card account number, and the like.

[0028] A "web service" as used herein refers to one or more software components, hardware components, or any combination thereof, associated with providing, receiving, and/or interfacing with data over a network.

[0029] FIG. 1 is a collaboration diagram of functional modules deployed on one or more computer systems for implementing secure access to PII data in accordance with an embodiment of the present invention. In one embodiment, a browser toolbar 102 includes a secure e-wallet 104 to securely access and store PII data. Browser toolbar 102 is in communication with a user toolbar interface 110 and a toolbar server application 112. Toolbar interface 110 translates the protocol used to communicate with browser toolbar 102. Particularly, user toolbar interface 110 interprets data requests received from browser toolbar 102 and passes each request to toolbar server application 112. Similarly, user toolbar interface 110 interprets responses from toolbar server application 112 and passes the interpreted response to browser toolbar 102.

[0030] Web services 114 is an interface between toolbar server application 112 and services such as customer account verification services 116, customer data access verification 118 and customer card and account information datastore 120. These services and interfaces can be associated with one or more card issuers, via web interface unit 106 and firewall unit 108.

[0031] Web services 114 controls operations between toolbar server application 112, customer account verification services 116, customer data access verification 118, and customer card and account information datastores 120.

[0032] The individual logic units of decisioning/orchestration units described above (*i.e.*, blocks 110-120) may be implemented in one or more computer systems or other processing systems, such as the secure information access system described below with respect to FIG. 2, for instance. In addition, units 110-120 can be operated and controlled by one or more card issuer systems, a third party system, or a combination of each.

[0033] Browser toolbar 102 is integrated within the user interface of a web browser residing on a customer's computer system. Web services initiated on the customer's system are analyzed by the browser tool bar unit 102 to detect a request for PII data. The browser tool bar unit 102 detects a PII data request based on the type of web service initiating the request or by analyzing the content within the request (*e.g.*, detecting an account number field).

[0034] As discussed above, transferring and managing PII data requires a higher level of security due to its confidential nature. Accordingly, after detecting a PII data request, browser toolbar 102 creates a public/private key pair which will be used to encrypt and transmit the requested PII data from web interface 106 to browser toolbar 102. Because the browser toolbar 102 resides on the customer's computer system, the public key is transmitted to toolbar server application 112 after creation. Preferably, the private key is not shared outside the browser toolbar unit 102. In this case, browser toolbar unit 102 is the sole unit which can decrypt the PII data received from web interface 106.

[0035] Creation of the public/private key pair is discussed further below with respect to FIG. 4. Preferably a distinct public/private key pair is generated to encrypt and transmit each respective PII data request.

[0036] Toolbar server application 112 inspects requests received from browser toolbar 102 to also determine when PII data is requested. PII data requests are detected by analyzing the type of web service making the request or the content of the request itself.

[0037] Upon detecting a PII data request from browser toolbar unit 102, toolbar server application 112 requests user credentials, *e.g.*, a username and password, from the customer. The customer is authenticated by verifying that the customer's user credentials correspond to a valid customer account record maintained by account verification services unit 116.

[0038] An authenticated customer is provided access to generic account data. Particularly, toolbar server application 112 will query customer card and account information datastore unit 120 for generic account data associated with the customer. More than one card may be associated with the customer. Upon a search of the records stored in customer card and account information datastore

unit 120, toolbar server application 112 determines all the cards associated with the customer that are eligible for use with the web service that initiated the PII data request at the customer's system.

[0039] Generic card data associated with each eligible card is sent to the customer's computer for presentation to the user. This data includes enough information for the customer to decipher one card from another upon presentation. Preferably, for each eligible card, the customer is presented generic card data that includes, for example, a picture associated with the card and the last 5 digits of the card. The customer may then select one or more cards presented for PII data download.

[0040] Before PII data can be downloaded, the toolbar application processing unit 114 verifies whether the customer has a high enough level of access privileges to access the PII data requested. Particularly, PII data access is granted after verifying card specific access credentials for each card the customer selected for PII data download. Accordingly, the customer is asked to enter card specific access credentials for each card selected.

[0041] Card specific access credentials include, for example, a security code unique to a particular card. The security code may be a 3 or 4 digit code printed on the card. Each security code number is verified by toolbar server application 112 with the records stored in a database of customer data access verification 118.

[0042] Once card specific access credentials are verified, PII data for each selected card can be downloaded to the browser toolbar 102. Toolbar application processing unit 114 retrieves the requested PII data from customer card and account information datastore 120. The retrieved PII data is encrypted using the public key previously received from the browser toolbar 102 and then transmitted to browser toolbar 102 via user toolbar interface 110 and web interface 106.

[0043] Because browser toolbar 102 maintains the private key required for decrypting the PII data, the customer's PII data is protected if it is intercepted by another unit external or internal to the customer's computer system during transmission to browser toolbar 102. After receipt of the encrypted PII data, browser toolbar 102 decrypts the PII data and stores it in secure e-wallet 104. The

customer can retrieve the stored PII data from secure e-wallet 104 to complete a transaction requiring entry of PII data.

[0044] In another embodiment, the public/private key pair created by browser toolbar 102 is used to encrypt/decrypt multiple PII data requests as opposed to distinct PII data requests as discussed above. Additionally, the public/private key pair created by browser toolbar 102 may be created prior to, during, or after detecting a PII data request.

[0045] In another embodiment, the PII data stored in secure e-wallet 104 is deleted upon the customer closing the current web browser session upon which the PII data was downloaded. Alternatively, the PII data may be deleted during or after the customer initiates a merchant based transaction that requires entry of the PII data.

[0046] In yet another embodiment, stored PII data may be updated as changes to customer card and account information datastore 120 occur via browser toolbar 102. These updates may occur at the request of the customer or at regularly scheduled intervals and times. Further, prior to a customer attempting to execute a transaction with a merchant using PII data stored in secure e-wallet 104, browser toolbar 102 can check to see if the PII data currently stored in the secure e-wallet 102 needs to be updated.

[0047] For instance, a customer's credit card may have expired since the PII data for the credit card was loaded into secure e-wallet 102 or a customer may have received a new credit card. In such cases, the PII data stored in the secure e-wallet 102 is updated to reflect the credit card's new expiration date or the existence of the new credit card. Access to updated PII data may require a similar authentication procedure discussed above to access the originally downloaded PII data. Particularly, the customer will again have to enter user access credentials and card specific access credentials for the particular card's PII data being updated. Similarly, the updated data will then be securely transmitted to the browser toolbar 102.

[0048] FIG. 2 illustrates a secure PII data access process 200, in accordance with an embodiment of the present invention. Generally, process 200 securely downloads PII card data from a secure information access system to a customer's

computer system. The secure information access system is preferably associated with one or more card issuers.

[0049] In block 201, a browser toolbar, such as browser toolbar 102, is created on the customer's computer system. Particularly, browser toolbar 102 is provided by one or more card issuers or another entity to the customer's computer system. Web services running on the customer's computer system are monitored by the browser toolbar to detect when PII data is requested. Upon detecting a PII data request, in block 202, browser toolbar 102 creates a public/private key pair to service the PII data request.

[0050] At block 203, the public key created by the browser toolbar is transmitted from the customer's computer system to one or more card processing servers at the secure information access system.

[0051] In addition to the public/private key creation in response to a PII data request, the customer is requested to provide user credentials to access a card issuer's web interface, as shown in block 204. For each card eligible for use with the web service that initiated the PII data request and which the customer wishes to access PII data for, in block 205 the customer is requested to provide card specific access credentials. After verifying the customer's user credentials and the card specific access credentials required to access the requested PII data, in block 206 the card processing servers will retrieve the requested PII data.

[0052] At block 207, the card processing servers encrypt the retrieved PII data using the public key previously sent in block 203. Encrypted PII data is then transmitted to the browser toolbar at the customer's computer system, block 208, for decryption, block 209, by the browser toolbar. The decrypted PII data is stored in an e-wallet, block 210, for use by the customer.

[0053] FIG. 3 illustrates the functional modules associated with securely downloading PII data to a customer's computer, according to one embodiment of the invention. Particularly, FIG. 3 is described with respect to the following entities and functional modules: e-wallet 302, browser toolbar 304, user 306, web and application services 308, security services 310, and data services 312. Modules 302-306 are associated with a customer's computer and modules 308-312 are associated with a card issuer.

[0054] Browser toolbar 304 creates an asymmetric private/public key pair which is used to encrypt one or more PII data transfers from/to the browser toolbar 304. Web and application services 308 receives a request from browser toolbar 304 to retrieve customer and account information, and detects a request for PII data.

[0055] The user 306 is then requested to input user credentials through his or her computing device. Web and application services 308 receives the user credentials and prepares a user verification request for security services unit 310. Security services 310, in turn, verifies the user credentials and notifies web and application services 308 whether the user credentials are legitimate. If the user credentials are not valid, an error message is presented to the user 306. If the user credentials are valid, web and application services 308 requests data services 312 to supply the customer and card data available for loading into browser toolbar 304. Web and application services 308 prepares the customer and card data for presentation and presents it to the user 306.

[0056] At this point, the user 306 has the opportunity to select the particular PII data, i.e., account data and card data, that the user 306 wishes to download into e-wallet 302. PII data may be associated with one or more accounts and cards. For each card selected, the user provides card specific access credentials. The card specific access credentials are received by web application services 308 which, in turn, prepares a data access verification request based on the card specific access credentials received.

[0057] Security services 310 verifies whether the card specific access credentials are legitimate. If the card specific access credentials are not legitimate, an error message is presented to user 306. If the card specific access credentials are legitimate, then web and application services 308 accesses the requested PII data and encrypts it with the public key previously created by browser toolbar 304. The encrypted data is transmitted to browser toolbar 304, which then decrypts the data and loads it into e-wallet 302.

[0058] FIG. 4 is a collaboration diagram of functional modules deployed on one or more computer systems for implementing public/private key pair creation in accordance with an embodiment of the present invention. Particularly, FIG. 4 is described with respect to the following entities and functional modules: random

number generator 401, browser toolbar 402, unique toolbar attributes 403, public/private key generation process 405, private key 406, public key 407, private key ring 408, public key ring 409, operating system and resources 410, and applications 411.

[0059] Browser toolbar 402 includes processes to create unique toolbar attributes 403 and unique user attributes 404. Public/private key generation process 405 uses any combination of inputs from random number generator 401, unique toolbar attributes 403, unique user attributes 404, applications 411, and other data sources for key pair creation. One or more key generation programs or algorithms can be used to take input from these various sources as desired.

[0060] Operating system and resources 410 communicates with browser toolbar 402 to initiate public/private key generation process 405. Public/private key generation process 405 seeks input from one or more sources (*e.g.*, 401, 403, 404, 411, etc.) based on a particular key generation program. These inputs are then input into the key calculation techniques of public/private key generation process 405 for the creation and output of private key 406 and public key 407. Private key 406 and public key 407 are unique to the particular browser toolbar 402 implementing public/private key generation process 405.

[0061] Private key 406 and public key 407 are stored as files along with a corresponding "key ring", private key ring 408 and public key ring 409, respectively. The stored private key 406 and private key ring 408 are accessible to the browser toolbar 402 for key retrieval and decryption as needed. The public key 407 and public key ring 409 may be publicly distributed as needed.

[0062] The present invention (*i.e.*, system 100, processes 200 and 300, or any part(s) or function(s) thereof) may be implemented using hardware, software or a combination thereof and may be implemented in one or more computer systems or other processing systems. However, the manipulations performed by the present invention were often referred to in terms, such as adding or comparing, which are commonly associated with mental operations performed by a human operator. No such capability of a human operator is necessary, or desirable in most cases, in any of the operations described herein which form part of the present invention. Rather, the operations are machine operations. Useful machines for performing the

operation of the present invention include general purpose digital computers or similar devices.

[0063] In fact, in one embodiment, the invention is directed toward one or more computer systems capable of carrying out the functionality described herein. An example of a computer system 500 is shown in FIG. 5.

[0064] The computer system 500 includes one or more processors, such as processor 504. The processor 504 is connected to a communication infrastructure 506 (*e.g.*, a communications bus, cross-over bar, or network). Various software embodiments are described in terms of this exemplary computer system. After reading this description, it will become apparent to a person skilled in the relevant art(s) how to implement the invention using other computer systems and/or architectures.

[0065] Computer system 500 can include a display interface 502 that forwards graphics, text, and other data from the communication infrastructure 506 (or from a frame buffer not shown) for display on the display unit 530.

[0066] Computer system 500 also includes a main memory 508, preferably random access memory (RAM), and may also include a secondary memory 510. The secondary memory 510 may include, for example, a hard disk drive 512 and/or a removable storage drive 514, representing a floppy disk drive, a magnetic tape drive, an optical disk drive, etc. The removable storage drive 514 reads from and/or writes to a removable storage unit 518 in a well known manner. Removable storage unit 518 represents a floppy disk, magnetic tape, optical disk, etc. which is read by and written to by removable storage drive 514. As will be appreciated, the removable storage unit 518 includes a computer usable storage medium having stored therein computer software and/or data.

[0067] In alternative embodiments, secondary memory 510 may include other similar devices for allowing computer programs or other instructions to be loaded into computer system 500. Such devices may include, for example, a removable storage unit 522 and an interface 520. Examples of such may include a program cartridge and cartridge interface (such as that found in video game devices), a removable memory chip (such as an erasable programmable read only memory (EPROM), or programmable read only memory (PROM)) and

associated socket, and other removable storage units 522 and interfaces 520, which allow software and data to be transferred from the removable storage unit 522 to computer system 500.

[0068] Computer system 500 may also include a communications interface 524. Communications interface 524 allows software and data to be transferred between computer system 500 and external devices. Examples of communications interface 524 may include a modem, a network interface (such as an Ethernet card), a communications port, a Personal Computer Memory Card International Association (PCMCIA) slot and card, etc. Software and data transferred via communications interface 524 are in the form of signals 528 which may be electronic, electromagnetic, optical or other signals capable of being received by communications interface 524. These signals 528 are provided to communications interface 524 via a communications path (*e.g.*, channel) 526. This channel 526 carries signals 528 and may be implemented using wire or cable, fiber optics, a telephone line, a cellular link, a radio frequency (RF) link and other communications channels.

[0069] In this document, the terms "computer program medium" and "computer usable medium" are used to generally refer to media such as removable storage drive 514, a hard disk installed in hard disk drive 512, and signals 528. These computer program products provide software to computer system 500. The invention is directed to such computer program products.

[0070] Computer programs (also referred to as computer control logic) are stored in main memory 508 and/or secondary memory 510. Computer programs may also be received via communications interface 524. Such computer programs, when executed, enable the computer system 500 to perform the features of the present invention, as discussed herein. In particular, the computer programs, when executed, enable the processor 504 to perform the features of the present invention. Accordingly, such computer programs represent controllers of the computer system 500.

[0071] In an embodiment where the invention is implemented using software, the software may be stored in a computer program product and loaded into computer system 500 using removable storage drive 514, hard drive 512 or

communications interface 524. The control logic (software), when executed by the processor 504, causes the processor 504 to perform the functions of the invention as described herein.

[0072] In another embodiment, the invention is implemented primarily in hardware using, for example, hardware components such as application specific integrated circuits (ASICs). Implementation of the hardware state machine so as to perform the functions described herein will be apparent to persons skilled in the relevant art(s).

[0073] In yet another embodiment, the invention is implemented using a combination of both hardware and software.

[0074] While various embodiments of the present invention have been described above, it should be understood that they have been presented by way of example, and not limitation. It will be apparent to persons skilled in the relevant art(s) that various changes in form and detail can be made therein without departing from the spirit and scope of the present invention. Thus, the present invention should not be limited by any of the above described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.

[0075] In addition, it should be understood that the figures and screen shots illustrated in the attachments, which highlight the functionality and advantages of the present invention, are presented for example purposes only. The architecture of the present invention is sufficiently flexible and configurable, such that it may be utilized (and navigated) in ways other than that shown in the accompanying figures.

[0076] Further, the purpose of the foregoing Abstract is to enable the U.S. Patent and Trademark Office and the public generally, and especially the scientists, engineers and practitioners in the art who are not familiar with patent or legal terms or phraseology, to determine quickly from a cursory inspection the nature and essence of the technical disclosure of the application. The Abstract is not intended to be limiting as to the scope of the present invention in any way. It is also to be understood that the steps and processes recited in the claims need not be performed in the order presented.

WHAT IS CLAIMED IS:

1. A method for securely downloading customer data to a browser toolbar comprising:

receiving, via the browser toolbar, a request for customer data from a customer;

determining the request for customer data includes a request for personal identifiable information requiring encryption by a public encryption key generated by the browser toolbar;

authenticating the customer based on a set of a user credential and an account specific access credential, wherein:

the user credential and the account specific access credential are distinct, and

the account specific access credential is associated with an account of the customer;

encrypting the requested personal identifiable information using the public encryption key generated by the browser toolbar; and

transmitting the encrypted personal identifiable information to the browser toolbar.

2. The method of claim 1, further comprising:

analyzing, by the browser toolbar, web services initiated on a computer system executing the browser toolbar;

detecting, based at least in part on the analyzing, when the request for customer data includes the request for personal identifiable information; and

creating a public/private key pair combination in response to the detecting.

3. The method of claim 1, wherein the account specific access credential includes a card security code associated with the customer.

4. The method of claim 1, further comprising:

determining the account is eligible for use with a web service initiating the request for customer data;

retrieving generic account data associated with the account, wherein the generic account data includes information for the customer to decipher the account from another; and

transmitting the generic account data to a computer system executing the browser toolbar.

5. The method of claim 4, wherein the generic account data includes a portion of an account number associated with the account.

6. The method of claim 4, further comprising:

receiving, via a user interface, a selection request indicating the customer requests access to personal identifiable information associated with the account; and

determining whether the customer has access to the personal identifiable information associated with the account based at least in part on the account specific access credential.

7. The method of claim 1, wherein the encrypted personal identifiable information is decrypted by the browser toolbar and stored in an e-wallet.

8. A system for securely integrating personal identifiable information with a browser toolbar unit, comprising:

a web interface unit configured to receive, via the browser toolbar, a request for customer data from a customer;

a toolbar server application configured to:

determine the request for customer data includes a request for personal identifiable information requiring encryption by a public encryption key generated by the browser toolbar;

authenticate the customer based on a set of a user credential and an account specific access credential, wherein:

the user credential and the account specific access credential are distinct, and

the account specific access credential is associated with an account of the customer; and

encrypt the requested personal identifiable information using the public encryption key generated by the browser toolbar; and

a transmission unit configured to transmit the encrypted personal identifiable information to the browser toolbar.

9. The apparatus of claim 8, wherein the browser toolbar unit is further configured to:

analyze web services initiated on a computer system executing the browser toolbar;

detect when the request for customer data includes the request for personal identifiable information; and

create a public/private key pair combination.

10. The apparatus of claim 8, wherein the account specific access credential includes a card security code associated with the customer.

11. The apparatus of claim 8, wherein the toolbar server application is further configured to:

determine the account is eligible for use with a web service initiating the request for customer data;

retrieve generic account data associated with the account, wherein the generic account data includes information for the customer to decipher the account from another; and

transmit, via the transmission unit, the generic account data to a computer system executing the browser toolbar.

12. The apparatus of claim 11, wherein the generic account data includes a portion of an account number associated with the account.

13. The apparatus of claim 11, wherein the toolbar server application is further configured to:

receive, via a user interface, a selection request indicating the customer requests access to personal identifiable information associated with the account; and

determine whether the customer has access to the personal identifiable information associated with the account based at least in part on the account specific access credential.

14. A computer-readable medium having stored thereon sequences of instruction, the sequences of instruction including instruction which when executed by a computer system causes the computer system to perform:

receiving, via the browser toolbar, a request for customer data from a customer;

determining the request for customer data includes a request for personal identifiable information requiring encryption by a public encryption key generated by the browser toolbar;

authenticating the customer based on a set of a user credential and an account specific access credential, wherein:

the user credential and the account specific access credential are distinct, and

the account specific access credential is associated with an account of the customer;

encrypting the requested personal identifiable information using the public encryption key generated by the browser toolbar; and

transmitting the encrypted personal identifiable information to the browser toolbar.

15. The computer-readable medium of Claim 14, further including a sequence of instruction which when executed by a computer system causes the computer system to perform:

analyzing, by the browser toolbar, web services initiated on a computer system executing the browser toolbar;

detecting, based at least in part on the analyzing, when the request for customer data includes the request for personal identifiable information; and

creating a public/private key pair combination in response to the detecting.

16. The computer-readable medium of Claim 14, wherein the account specific access credential includes a card security code associated with the customer.

17. The computer-readable medium of Claim 14, further including a sequence of instruction which when executed by a computer system causes the computer system to perform:

determining the account is eligible for use with a web service initiating the request for customer data;

retrieving generic account data associated with the account, wherein the generic account data includes information for the customer to decipher the account from another; and

transmitting the generic account data to a computer system executing the browser toolbar.

18. The computer-readable medium of Claim 17, wherein the generic account data includes a portion of an account number associated with the account.

19. The computer-readable medium of Claim 14, further including a sequence of instruction which when executed by a computer system causes the computer system to perform:

receiving, via a user interface, a selection request indicating the customer requests access to personal identifiable information associated with the account; and

determining whether the customer has access to the personal identifiable information associated with the account based at least in part on the account specific access credential.

20. The computer-readable medium of Claim 14, wherein the encrypted personal identifiable information is decrypted by the browser toolbar and stored in an e-wallet.

ABSTRACT

Customer data is securely downloaded to a browser toolbar by performing a check to determine whether a request for customer data includes a request for personal identifiable information requiring encryption by a public encryption key generated by the browser toolbar. The customer is authenticated based on a set of a user credential and an account specific access credential. The account specific access credential is associated with the account of the customer. Requested personal identifiable information is encrypted using the public encryption key generated by the browser toolbar. Encrypted personal identifiable information is transmitted to the browser toolbar.

Fitzpatrick, Cella, Harper, & Scinto
30 Rockefeller Plaza
New York, New York 10112
212-218-2100

Title: Securely Accessing Account Data
Inventor: William J. Gray
Attorney Docket No. 03292.102760

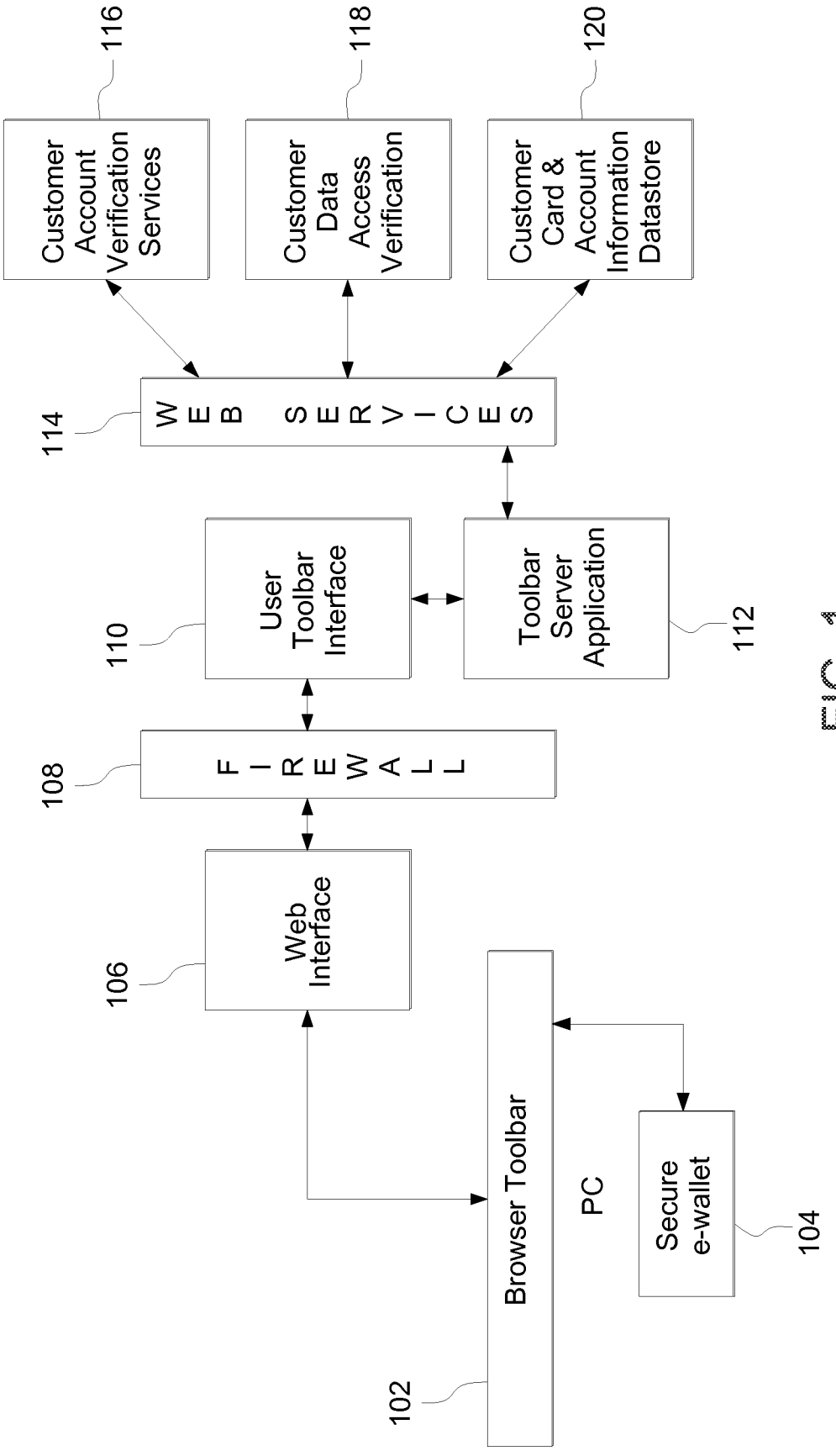

FIG. 1 100

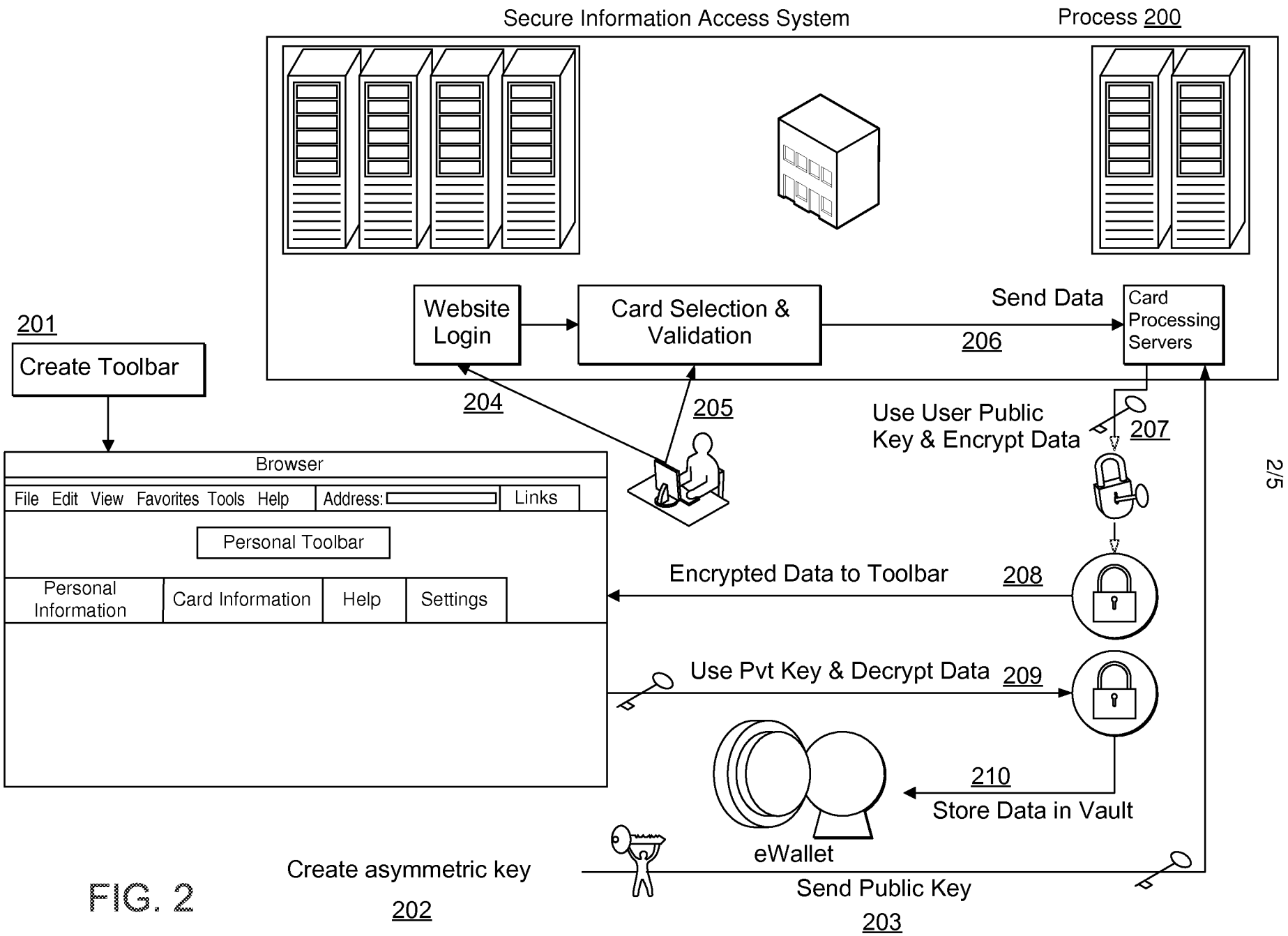

FIG. 2

Fitzpatrick, Cella, Harper, & Scinto
30 Rockefeller Plaza
New York, New York 10112
212-218-2100

Title: Securely Accessing Account Data
Inventor: William J. Gray
Attorney Docket No. 03292.102760

Fitzpatrick, Cella, Harper, & Scinto
30 Rockefeller Plaza
New York, New York 10112
212-218-2100

Title: Securely Accessing Account Data
Inventor: William J. Gray
Attorney Docket No. 03292.102760

300

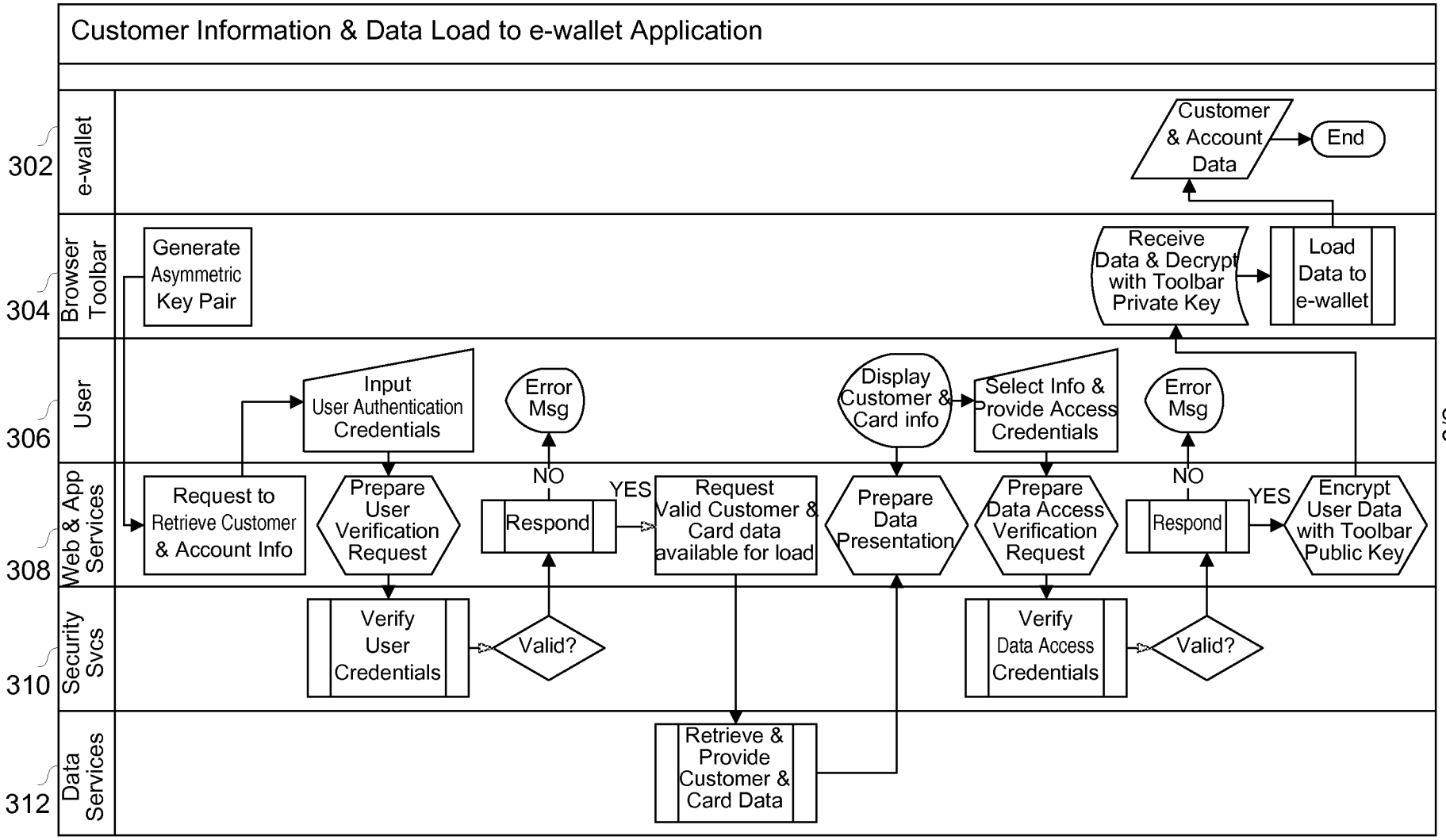

FIG. 3

Fitzpatrick, Cella, Harper, & Scinto
30 Rockefeller Plaza
New York, New York 10112
212-218-2100

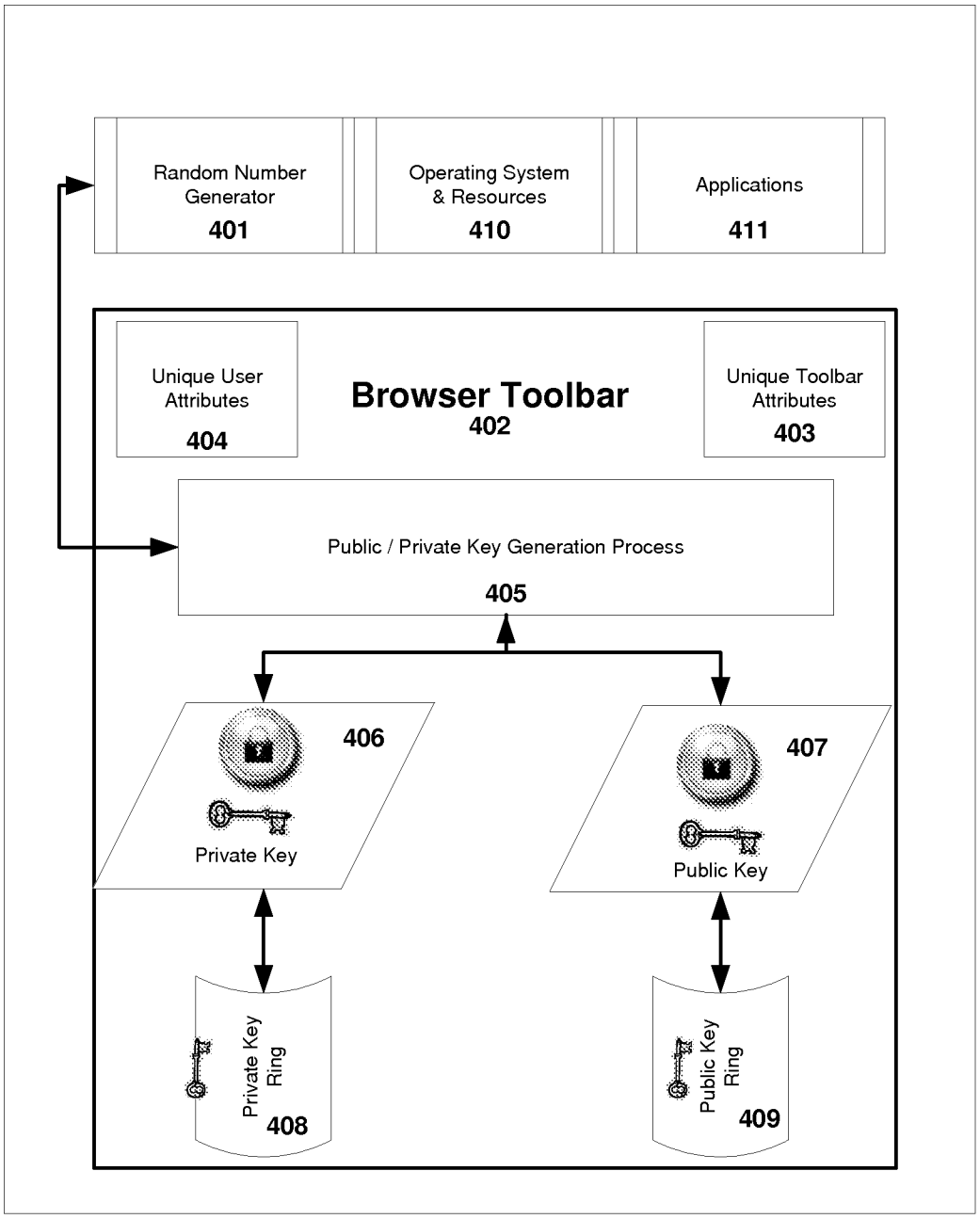

Fig. 4

400

Create Browser Toolbar Key Pair

Fitzpatrick, Cella, Harper, & Scinto
30 Rockefeller Plaza
New York, New York 10112
212-218-2100

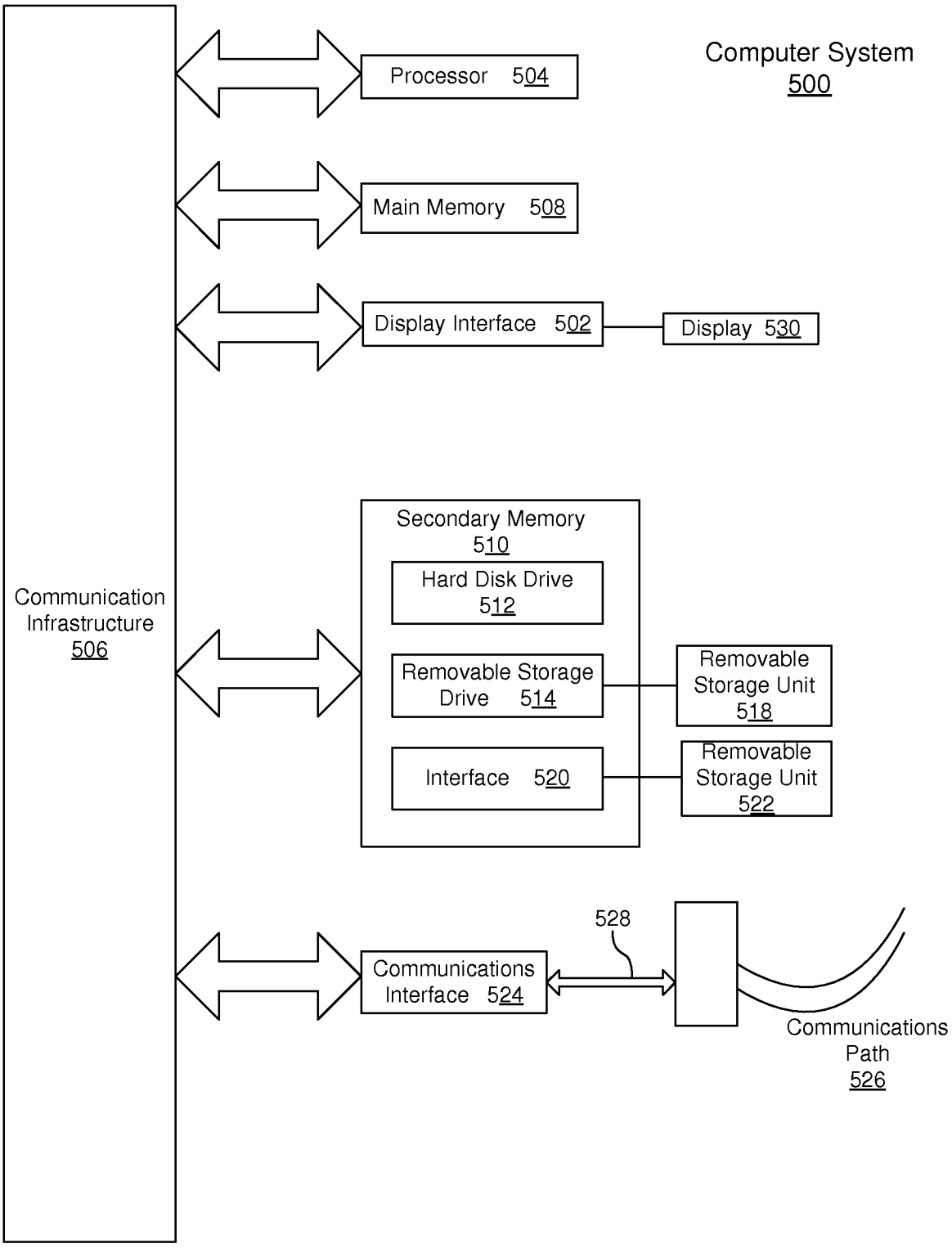

FIG. 5

PTO/SB/14 (07-07)
Approved for use through 06/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	03292.102760.
	Application Number	
Title of Invention	METHODS, APPARATUS AND COMPUTER PROGRAM PRODUCTS FOR SECURELY ACCESSING ACCOUNT DATA	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Applicant Information:

Applicant 1 Remove

Applicant Authority ◉ Inventor ○ Legal Representative under 35 U.S.C. 117 ○ Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
	William	J	Gray	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Peoria	State/Province	AZ	Country of Residence i	US

Citizenship under 37 CFR 1.41(b) i: US

Mailing Address of Applicant:

Address 1	American Express, General Counsel's Office
Address 2	3 World Financial Center, 200 Vesey Street

City	New York	State/Province	NY
Postal Code	10285	Country i	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	66569		
Email Address		Add Email	Remove Email

Application Information:

Title of the Invention	METHODS, APPARATUS AND COMPUTER PROGRAM PRODUCTS FOR SECURELY ACCESSING ACCOUNT DATA		
Attorney Docket Number	03292.102760.	Small Entity Status Claimed	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		Sub Class (if any)	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)	5	Suggested Figure for Publication (if any)	

PTO/SB/14 (07-07)
Approved for use through 06/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	03292.102760.
	Application Number	
Title of Invention	METHODS, APPARATUS AND COMPUTER PROGRAM PRODUCTS FOR SECURELY ACCESSING ACCOUNT DATA	

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Enter either Customer Number or complete the Representative Name section below. If both sections are completed the Customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	66569		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	61138711	2008-12-18

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).

Remove

Application Number	Country [i]	Parent Filing Date (YYYY-MM-DD)	Priority Claimed
			○ Yes ○ No

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Assignee Information:

Providing this information in the application data sheet does not substitute for compliance with any requirement of part 3 of Title 37 of the CFR to have an assignment recorded in the Office.

Assignee 1 Remove

PTO/SB/14 (07-07)
Approved for use through 06/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	03292.102760.
	Application Number	
Title of Invention	METHODS, APPARATUS AND COMPUTER PROGRAM PRODUCTS FOR SECURELY ACCESSING ACCOUNT DATA	

If the Assignee is an Organization check here. ☒			
Organization Name	American Express Travel Related Services Company, Inc.		
Mailing Address Information:			
Address 1	American Express, General Counsel's Office		
Address 2	3 World Financial Center		
City	New York	**State/Province**	NY
Country [i]	US	Postal Code	10285
Phone Number		Fax Number	
Email Address			
Additional Assignee Data may be generated within this form by selecting the **Add** button.		Add	

Signature:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/Leonard P Diana/			Date (YYYY-MM-DD)	2009-07-30
First Name	Leonard P.	Last Name	Diana	Registration Number	29296

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	METHODS, APPARATUS AND COMPUTER PROGRAM PRODUCTS FOR SECURELY ACCESSING ACCOUNT DATA
First Named Inventor/Applicant Name:	William J Gray
Filer:	Jonathan Berschadsky/DAVID NGUY
Attorney Docket Number:	03292.102760.

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility application filing	1011	1	330	330
Utility Search Fee	1111	1	540	540
Utility Examination Fee	1311	1	220	220
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**1090**

Electronic Acknowledgement Receipt

EFS ID:	5802410
Application Number:	12512873
International Application Number:	
Confirmation Number:	6515
Title of Invention:	METHODS, APPARATUS AND COMPUTER PROGRAM PRODUCTS FOR SECURELY ACCESSING ACCOUNT DATA
First Named Inventor/Applicant Name:	William J Gray
Customer Number:	66569
Filer:	Jonathan Berschadsky/DAVID NGUY
Filer Authorized By:	Jonathan Berschadsky
Attorney Docket Number:	03292.102760.
Receipt Date:	30-JUL-2009
Filing Date:	
Time Stamp:	19:04:28
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1090
RAM confirmation Number	4729
Deposit Account	503939
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		SPEC03292102760.pdf	94495 c5b651b92088a7147bccd9d4e317c91e4c323391	yes	23

	Multipart Description/PDF files in .zip description		
	Document Description	Start	End
	Specification	1	16
	Claims	17	22
	Abstract	23	23

Warnings:					
Information:					
2	Drawings-only black and white line drawings	DRWS03292102760.pdf	102365 c21735bc4f6a7cf0ac44b4f2112a21045da79eda	no	5
Warnings:					
Information:					
3	Application Data Sheet	ADS03292102760.pdf	841266 0fcb50a82694db5d07d02eb44b9eed177a75b9fa	no	6
Warnings:					
Information:					
4	Fee Worksheet (PTO-875)	fee-info.pdf	33325 5ec850d91de8548241badb3d248e7df3fcdcc400	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1071451		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.